PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-023137
(43)Date of publication of application : 21.01.2000

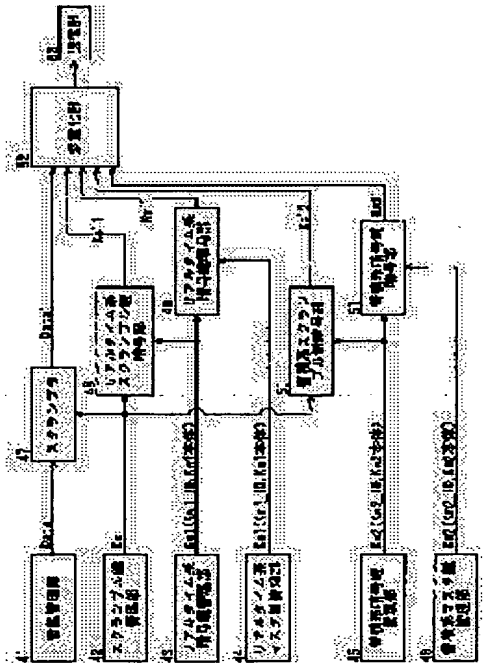
(51)Int.Cl. H04N 7/167
H04H 1/00
H04L 9/08
H04L 9/14

(21)Application number : 10-201090
(22)Date of filing : 02.07.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MASUDA ISAO
GOTO YOSHIMASA
HARADA TAKENOSUKE
MACHIDA KAZUHIRO
KATAOKA MITSUTERU

(54) BROADCASTING SYSTEM AND BROADCASTING TRANSMITTER- RECEIVER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a broadcasting system capable of preventing the fraudulent viewing of stored program data.
SOLUTION: In this broadcasting system by which a program is broadcasted on the side of transmission, the program is viewed on the side of reception in real time or stored, reproduced later and viewed, a scramble key 42 for descrambling program data 451 is transmitted on the side of transmission while being enciphered through plural kinds of cryptographic keys 43 and 45 at different updating intervals by enciphering parts 48 and 50, and when storing the broadcasting program, on the side of reception, the scrambled program data are stored corresponding to the scramble key enciphered by the cryptographic key at short updating intervals. Even when the cryptographic key is fraudulently deciphered, the condition of viewing all the stored programs can be prevented.



LEGAL STATUS

[Date of request for examination] 21.02.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3565715

[Date of registration] 18.06.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－23137
（P2000－23137A）
(43)公開日　平成12年１月21日(2000.1.21)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167		５Ｃ０６４
Ｈ０４Ｈ　1/00		Ｈ０４Ｈ　1/00	Ｆ	５Ｋ０１３
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ	
9/14			６４１	

審査請求　未請求　請求項の数18　ＦＤ　（全 13 頁）

(21)出願番号　特願平10－201090

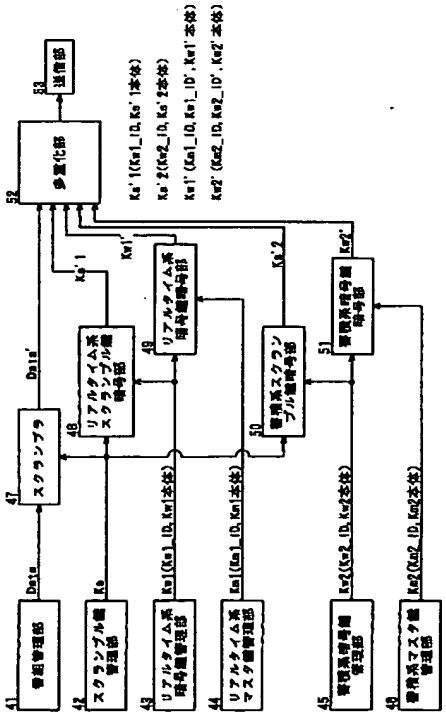
(22)出願日　平成10年７月２日(1998.7.2)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　増田　功
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　後藤　吉正
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100099254
弁理士　役　昌明　（外３名）

最終頁に続く

(54)【発明の名称】　放送システムと放送送受信装置

(57)【要約】
【課題】　蓄積された番組データの不正視聴を防ぐことができる放送システムを提供する。
【解決手段】　送信側が番組を放送し、受信側が、この番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムにおいて、送信側では、番組データ41のスクランブルを解くスクランブル鍵42を、更新間隔を異にする複数種類の暗号鍵43、45で暗号部48、50で暗号化して送信し、受信側では、放送番組を蓄積するとき、スクランブルされた番組データと、更新間隔が短い暗号鍵で暗号化されたスクランブル鍵とを対応付けて蓄積する。暗号鍵が不正に解かれた場合でも、蓄積されている番組の全てが視聴可能になってしまう事態を防ぐことができる。



1

【特許請求の範囲】

【請求項１】　送信側が番組を放送し、受信側が、この番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムにおいて、

送信側では、番組データのスクランブルを解くスクランブル鍵を複数種類の暗号鍵で暗号化し、前記暗号鍵の各々を暗号化して送信し、

受信側では、暗号化された複数種類の暗号鍵を復号化して保持し、蓄積した番組を再生して視聴する場合に、リアルタイムで番組を視聴するときに用いる暗号鍵とは異なる暗号鍵を用いて蓄積されたスクランブル鍵を復号化し、復号化した前記スクランブル鍵を用いて蓄積された番組データのスクランブルを解除することを特徴とする放送システム。

【請求項２】　送信側では、前記複数種類の暗号鍵の更新間隔を違えて、暗号化した前記複数種類の暗号鍵を送信し、受信側では、リアルタイムで番組を視聴するときに用いる暗号鍵より更新間隔が短い暗号鍵を、蓄積した番組の視聴のために用いることを特徴とする請求項１に記載の放送システム。

【請求項３】　送信側では、リアルタイムで番組を視聴するときに用いる暗号鍵を第１の種類のマスタ鍵で暗号化し、蓄積した番組を視聴するときに用いる暗号鍵を第２の種類のマスタ鍵で暗号化することを特徴とする請求項１または２に記載の放送システム。

【請求項４】　送信側では、蓄積した番組を視聴するときに用いる前記暗号鍵を番組ごとに更新することを特徴とする請求項２または３に記載の放送システム。

【請求項５】　受信側では、リアルタイムで番組を視聴するときに用いる暗号鍵を前記第１の種類のマスタ鍵で復号化して保持し、放送番組をリアルタイムで視聴するときには、復号化した前記暗号鍵を用いて、暗号化されたスクランブル鍵を復号化し、復号化した前記スクランブル鍵を用いて番組データのスクランブルを解除することを特徴とする請求項１乃至４に記載の放送システム。

【請求項６】　受信側では、蓄積した番組を視聴するときに用いる暗号鍵を前記第２の種類のマスタ鍵で復号化して保持し、蓄積した番組を再生して視聴するときには、復号化した前記暗号鍵を用いて、蓄積されている暗号化されたスクランブル鍵を復号化し、復号化した前記スクランブル鍵を用いて再生する番組データのスクランブルを解除することを特徴とする請求項１乃至４に記載の放送システム。

【請求項７】　送信側では、前記第２の種類のマスタ鍵を前記第１の種類のマスタ鍵で暗号化して送信することを特徴とする請求項３に記載の放送システム。

【請求項８】　受信側では、暗号化されて送られて来る前記第２の種類のマスタ鍵を前記第１の種類のマスタ鍵で復号化して保持することを特徴とする請求項７に記載の放送システム。

2

【請求項９】　前記第１の種類のマスタ鍵が、各受信側に個別に設定され、前記第２の種類のマスタ鍵が、各受信側に共通に設定されることを特徴とする請求項３、５、６、７または８に記載の放送システム。

【請求項１０】　受信側が放送番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムの送信装置において、

第１の種類の暗号鍵を生成管理する第１の暗号鍵管理手段と、

第２の種類の暗号鍵を生成管理する第２の暗号鍵管理手段と、

番組データを暗号化したスクランブル鍵を、前記第１の種類の暗号鍵で暗号化する第１のスクランブル鍵暗号化手段と、

番組データを暗号化したスクランブル鍵を、前記第２の種類の暗号鍵で暗号化する第２のスクランブル鍵暗号化手段と、

前記第１の種類の暗号鍵を第１の種類のマスタ鍵で暗号化する第１の暗号鍵暗号化手段と、

前記第２の種類の暗号鍵を第２の種類のマスタ鍵で暗号化する第２の暗号鍵暗号化手段と、

第１のスクランブル鍵暗号化手段で暗号化されたスクランブル鍵、第２のスクランブル鍵暗号化手段で暗号化されたスクランブル鍵、第１の暗号鍵暗号化手段で暗号化された暗号鍵、第２の暗号鍵暗号化手段で暗号化された暗号鍵、及びスクランブル鍵で暗号化された番組データを多重化して送信する送信手段とを備えることを特徴とする送信装置。

【請求項１１】　前記第２の暗号鍵管理手段が生成管理する第２の種類の暗号鍵の更新期間が、前記第１の暗号鍵管理手段が生成管理する第１の種類の暗号鍵の更新期間より短いことを特徴とする請求項１０に記載の送信装置。

【請求項１２】　前記第２の種類のマスタ鍵を前記第１の種類のマスタ鍵で暗号化するマスタ鍵暗号化手段を具備し、前記マスタ鍵暗号化手段で暗号化されたマスタ鍵を前記送信手段を通じて送信することを特徴とする請求項１０に記載の送信装置。

【請求項１３】　前記第１の種類のマスタ鍵を各受信装置ごとに設定し、前記第２の種類のマスタ鍵を各受信装置に共通に設定することを特徴とする請求項１０または１２に記載の送信装置。

【請求項１４】　送信装置から放送された番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムの受信装置において、

暗号化されている第１の種類の暗号鍵を、第１の種類のマスタ鍵を用いて復号化する第１の暗号鍵復号手段と、

暗号化されている第２の種類の暗号鍵を、第２の種類のマスタ鍵を用いて復号化する第２の暗号鍵復号手段と、

スクランブル鍵で暗号化された番組データと前記第２の

種類の暗号鍵で暗号化されたスクランブル鍵とを記憶する蓄積手段と、
前記第１の暗号鍵復号手段で復号化された暗号鍵を用いて、現在の受信情報に含まれる暗号化されたスクランブル鍵を復号化する第１のスクランブル鍵復号手段と、
前記第２の暗号鍵復号手段で復号化された暗号鍵を用いて、前記蓄積手段から読み出した暗号化されているスクランブル鍵を復号化する第２のスクランブル鍵復号手段と、
前記第１のスクランブル鍵復号手段または第２のスクランブル鍵復号手段で復号化されたスクランブル鍵を用いて番組データをデスクランブルするデスクランブラとを備えることを特徴とする受信装置。
【請求項１５】　前記第２の暗号鍵復号手段で復号化される第２の種類の暗号鍵の更新期間が、前記第１の暗号鍵復号手段で復号化される第１の種類の暗号鍵の更新期間より短いことを特徴とする請求項１４に記載の受信装置。
【請求項１６】　前記デスクランブラが、番組をリアルタイム視聴するときには、現在受信しているスクランブルされている番組データを、前記第１のスクランブル鍵復号手段で復号されたスクランブル鍵を用いてデスクランブルし、蓄積された番組を再生して視聴するときには、前記蓄積手段から読み出したスクランブルされている番組データを、前記第２のスクランブル鍵復号手段で復号されたスクランブル鍵を用いてデスクランブルすることを特徴とする請求項１４に記載の受信装置。
【請求項１７】　暗号化されている前記第２の種類のマスタ鍵を、前記第１の種類のマスタ鍵を用いて復号化するマスタ鍵復号手段を具備し、前記マスタ鍵復号手段で復号化されたマスタ鍵を保持することを特徴とする請求項１４に記載の受信装置。
【請求項１８】　前記第１の種類のマスタ鍵が、各受信装置ごとに設定され、前記第２の種類のマスタ鍵が、各受信装置に共通に設定されることを特徴とする請求項１４または１７に記載の受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、受信側での放送番組の蓄積を可能にした放送システムと、このシステムで使用する放送送受信装置に関し、特に、蓄積した番組の不正視聴を防止するものである。
【０００２】
【従来の技術】有料放送では、スクランブルを掛けた番組が放送され、受信契約が有効な場合に、受信装置でスクランブルを解除するデスクランブルが可能となる。
【０００３】有料放送での暗号化は、３種類の鍵を用いて行なわれる。番組の映像音声情報はスクランブル鍵（Ｋｓ）でスクランブルされ、このスクランブル鍵が暗号鍵（Ｋｗ）で暗号化される。また、暗号鍵はマスター鍵（Ｋｍ）で暗号化されて受信装置に送信される。
【０００４】スクランブル鍵（Ｋｓ）は１秒程度の短い周期で更新される各受信装置に共通の鍵である。また、暗号鍵（Ｋｗ）は各受信装置に個別に割り当てられる鍵であり、受信契約が交わされると、この暗号鍵がマスター鍵で暗号化されて放送局から受信装置に送信され、また、約１年ごとの受信契約の更新に合わせて、新たな暗号鍵がマスター鍵で暗号化されて放送局から受信装置に送信される。
【０００５】マスター鍵（Ｋｍ）は、受信装置ごとに異なり、各受信装置のセキュリティモジュールに記憶されている。このセキュリティモジュールは、こうした暗号解読用の鍵などの秘密情報や個人ＩＤなどを記憶するＩＣカードで構成され、放送局から送られて来たものが受信装置にセットされる。
【０００６】従来の送信装置は、図５に示すように、番組データ（Data）を生成し管理する番組管理部11と、Dataを暗号化するためのスクランブル鍵Ｋｓを生成し管理するスクランブル鍵管理部12と、Ｋｓを暗号化するための暗号鍵Ｋｗを、その識別子（Kw_ID）と共に生成管理する暗号鍵管理部13と、Ｋｗを暗号化するためのマスタ鍵Ｋｍを、その識別子（Km_ID）と共に生成し管理するマスタ鍵管理部14と、DataをＫｓでスクランブルしスクランブル化された番組データData'を出力するスクランブラ15と、Ｋｗの鍵本体を使ってＫｓを暗号化し、暗号化スクランブル鍵Ｋｓ'を出力するスクランブル鍵暗号部16と、Ｋｍの鍵本体を使ってＫｗを暗号化し、暗号化暗号鍵Ｋｗ'を出力する暗号鍵暗号部17と、Data'、Ｋｓ'及びＫｗ'を多重化し、多重化情報として出力する多重化部18と、多重化情報を伝送情報に変換して送信する送信部19とを備えている。
【０００７】この装置では、番組管理部11で生成されたDataが、スクランブラ15でスクランブル鍵Ｋｓを使ってスクランブルされ、スクランブル化された番組データData'が多重化部18に出力される。また、このＫｓは、暗号鍵管理部13で生成されたＫｗで暗号化される。
【０００８】暗号鍵管理部13では、生成する暗号鍵の識別子Kw_IDに、２ｂｙｔｅ長のビット配列で、Ｋｗ本体を一意に示す値を割り当て、暗号鍵をＫｗ(Kw_ID、Ｋｗ本体）の形式で生成管理している。
【０００９】スクランブル鍵暗号部16は、Dataのスクランブルで用いたＫｓを、暗号鍵管理部13から出力されたＫｗの鍵本体を使って暗号化し、暗号化に用いたＫｗのKw_IDを付加して、暗号化スクランブル鍵をＫｓ'（Kw_ID、Ｋｓ'本体）の形式で多重化部18に出力する。また、このＫｗは、マスタ鍵管理部14で生成されたＫｍで暗号化される。
【００１０】マスタ鍵管理部14では、生成したマスタ鍵を、識別子と共に、Ｋｍ(Km_ID、Ｋｍ本体）の形式で管理している。

【００１１】暗号鍵暗号部17は、契約の更新時期に、Ｋｍの鍵本体を使ってＫｗ(Kw_ID、Ｋｗ本体）を暗号化し、暗号化に用いたＫｍのKm_IDを付加して、暗号化暗号鍵をＫｗ'(Km_ID、Kw_ID'、Ｋｗ'本体）の形式で多重化部18に出力する。

【００１２】多重化部18は、入力するData'、Ｋｓ'(Kw_ID、Ｋｓ'本体）及びＫｗ'(Km_ID、Kw_ID'、Ｋｗ'本体）を多重化して、その多重化情報を送信部19に出力し、送信部19は、それを伝送情報に変換して送信する。

【００１３】一方、受信装置は、契約時またはその更新時に送られてくる暗号化された暗号鍵を、マスタ鍵で復号化して保持し、この暗号鍵を用いて、暗号化されているスクランブル鍵を復号化し、復号化したスクランブル鍵を用いて番組の映像音声情報のデスクランブルを行なう。

【００１４】ところで、特開平１０－１１８９４公報や特開平８－１４９４４９公報には、放送番組のリアルタイムでの視聴が可能であるとともに、放送番組を蓄積し、都合の良いときに再生して視聴できる放送システムが提案されている。

【００１５】こうしたシステムの場合、受信装置で放送番組をリアルタイムで視聴するときには、通常の受信の場合と同様に、受信契約が有効であれば、有料番組のスクランブルは解除され、受信契約が無効であれば、スクランブルは解除されない。また、蓄積された番組を視聴するときも同じであって、その視聴時点で受信契約が有効であれば、視聴する有料番組のスクランブルは解除され、受信契約が無効であれば、スクランブルは解除されない。

【００１６】この受信装置の構成を図６に示している。この装置は、受信した伝送情報を多重情報に変換して出力するチューナー21と、チューナー21から出力された多重化情報を暗号化番組データData'、暗号化スクランブル鍵Ｋｓ'及び暗号化暗号鍵Ｋｗ'に分離して出力する分離部22と、Data'を蓄積する番組データ蓄積部24とＫｓ'を蓄積するスクランブル鍵蓄積部25とを具備する蓄積媒体36と、分離部22で分離されたData'とＫｓ'とを対応をとって番組データ蓄積部24及びスクランブル鍵蓄積部25に書き込む書き込み管理部23と、蓄積されているData'とＫｓ'とを番組データ蓄積部24及びスクランブル鍵蓄積部25から取り出して出力する読み込み管理部26と、リアルタイムで視聴するときは分離部22からData'を選択し、蓄積された番組を視聴するときは読み込み管理部26からData'を選択する番組データ選択部27と、リアルタイムで視聴するときは分離部22からＫｓ'を選択し、蓄積された番組を視聴するときは読み込み管理部26からＫｓ'を選択するスクランブル鍵選択部28と、マスタ鍵Ｋｍを蓄積しているマスタ鍵蓄積部30と、Ｋｍを使ってＫｗ'を復号化し、復号化されたＫｗを出力する暗号鍵復号部29と、暗号鍵復号部29から入力するＫｗを蓄積管理する暗号鍵管理部31と、スクランブル鍵選択部28から入力するＫｓ'を暗号鍵管理部31から取り出したＫｗで復号化するスクランブル鍵復号部32と、番組データ選択部27から入力するData'をスクランブル鍵復号部32から入力するＫｓで復号化し、復号化したDataを出力するデスクランブラ33と、Dataを再生信号にデコードするデコーダ34と、再生信号に基づいて番組表示を行なう表示装置35とを備えている。また、マスタ鍵蓄積部30、暗号鍵復号部29、暗号鍵管理部31、及びスクランブル鍵復号部32はセキュリティモジュール37に設けられている。

【００１７】この受信装置では、分離部22が、チューナー21から入力する多重化情報を、暗号化番組データData'、暗号化スクランブル鍵Ｋｓ'(Kw_ID、Ｋｓ'本体）及び暗号化暗号鍵Ｋｗ'(Km_ID、Kw_ID'、Ｋｗ'本体）に分離して出力する。書き込み管理部23は、分離部22から分離されたData'とＫｓ'とを対応をとって蓄積媒体36の番組データ蓄積部24及びスクランブル鍵蓄積部25に書き込む。

【００１８】また、暗号鍵復号部29は、マスタ鍵蓄積部30に蓄積されたマスタ鍵Ｋｍ(Km_ID、Ｋｍ本体）と同一のKm_IDをもつ暗号化暗号鍵Ｋｗ'(Km_ID、Kw_ID'、Ｋｗ'本体）が分離部22から出力されたとき、そのＫｍを使ってＫｗ'を復号化し、復号化暗号鍵Ｋｗ(Kw_ID、Ｋｗ本体）を暗号鍵管理部31に出力する。暗号鍵管理部31は、これを蓄積管理する。

【００１９】視聴者からリアルタイムの番組視聴が指示された場合には、番組データ選択部27は、分離部22からData'を入手してデスクランブラ33に出力し、番組データ選択部27と連動するスクランブル鍵選択部28は、分離部22から暗号化スクランブル鍵Ｋｓ'(Kw_ID、Ｋｓ'本体）を入手してスクランブル鍵復号部32に出力する。

【００２０】スクランブル鍵復号部32は、スクランブル鍵選択部28からＫｓ'(Kw_ID、Ｋｓ'本体）が入力すると、暗号鍵管理部31からＫｓ'と同一のKw_IDを持つＫｗ（Kw_ID、Ｋｗ本体）を取り出し、それを使ってＫｓ'を復号化する。復号化されたＫｓはデスクランブラ33に出力され、デスクランブラ33は、このＫｓを使って番組データ選択部27から入力するData'を復号化し、復号化したDataをデコーダ34に出力する。

【００２１】こうして、有料番組のリアルタイムの視聴が可能となる。

【００２２】一方、視聴者から蓄積番組の視聴が指示された場合には、読み込み管理部26は、番組データ蓄積部24から、蓄積されている指示された番組のData'を読み出すとともに、そのData'のスクランブルを行なっているＫｓ'(Kw_ID、Ｋｓ'本体）をスクランブル鍵蓄積部25から取り出す。

【００２３】番組データ選択部27は、読み込み管理部26からData'を入手してデスクランブラ33に出力し、番組データ選択部27と連動するスクランブル鍵選択部28は、

読み込み管理部26から暗号化スクランブル鍵Ｋｓ'(Kw_ID、Ｋｓ'本体）を入手してスクランブル鍵復号部32に出力する。

【００２４】その後の動作は、リアルタイム視聴の場合と同じである。こうして、蓄積された有料番組の視聴が可能となる。

【００２５】

【発明が解決しようとする課題】しかし、この蓄積型放送システムでは、暗号鍵Ｋｗの更新周期が約１年であるため、受信装置の蓄積媒体36には、同一の暗号鍵Ｋｗで暗号化されたスクランブル鍵Ｋｓ'によりスクランブルされている番組が多数蓄積されることになり、暗号鍵Ｋｗが不正に解かれた場合、その暗号鍵で、それらの蓄積されている全ての番組データが不正に視聴できてしまうという問題点を有している。

【００２６】この点は、暗号鍵Ｋｗの更新周期を短縮すれば解消できるが、しかし、暗号鍵Ｋｗを暗号化するマスタ鍵Ｋｍは各受信装置ごとに異なっているので、何１０万台にも及ぶ受信装置のそれぞれのマスタ鍵Ｋｍで暗号鍵Ｋｗを暗号化するのに多くの時間が掛かり、短い間隔で暗号鍵Ｋｗを更新することは実際上できない。

【００２７】本発明は、こうした点の改善を図るものであり、蓄積された番組データの不正視聴を防止する放送システムを提供し、また、その放送システムを実現する放送送信装置と放送受信装置とを提供することを目的としている。

【００２８】

【課題を解決するための手段】そこで、本発明の放送システムでは、スクランブル鍵を暗号化する暗号鍵として、複数種類の暗号鍵を用意し、番組をリアルタイムで視聴するときにスクランブル鍵を復号化する暗号鍵と、蓄積した番組を再生して視聴するときにスクランブル鍵を復号化する暗号鍵との種類を違えている。

【００２９】また、蓄積した番組を視聴するときに用いる暗号鍵の更新間隔を、リアルタイムで番組を視聴するときに用いる暗号鍵の更新間隔より短く設定している。

【００３０】このように、蓄積した番組の視聴に、リアルタイム視聴の場合と異なる種類の暗号鍵を使用し、また、その暗号鍵を短い間隔で更新することにより、暗号鍵が不正に解かれた場合の被害を極小化することができ、蓄積された番組が広く不正視聴されてしまう事態を防止することができる。

【００３１】

【発明の実施の形態】本発明の請求項１に記載の発明は、送信側が番組を放送し、受信側が、この番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムにおいて、送信側では、番組データのスクランブルを解くスクランブル鍵を複数種類の暗号鍵で暗号化し、その暗号鍵の各々を暗号化して送信し、受信側では、暗号化された複数種類の暗号鍵を復号化して保持し、蓄積した番組を再生して視聴する場合に、リアルタイムで番組を視聴するときに用いる暗号鍵とは異なる暗号鍵を用いて蓄積されたスクランブル鍵を復号化し、復号化したスクランブル鍵を用いて蓄積された番組データのスクランブルを解除するようにしたものであり、複数種類の暗号鍵を用いることにより、暗号鍵が不正解読された場合の被害の範囲を狭めることができる。

【００３２】請求項２に記載の発明は、送信側では、複数種類の暗号鍵の更新間隔を違えて、暗号化した複数種類の暗号鍵を送信し、受信側では、リアルタイムで番組を視聴するときに用いる暗号鍵より更新間隔が短い暗号鍵を、蓄積した番組の視聴のために用いるようにしたものであり、暗号鍵が不正に解かれた場合でも、蓄積されている番組の全てが視聴可能になってしまう事態を防ぐことができる。

【００３３】請求項３に記載の発明は、送信側では、リアルタイムで番組を視聴するときに用いる暗号鍵を第１の種類のマスタ鍵で暗号化し、蓄積した番組を視聴するときに用いる暗号鍵を第２の種類のマスタ鍵で暗号化するようにしたものであり、蓄積番組の視聴に用いる暗号鍵を、リアルタイム視聴に用いる暗号鍵とは異なる態様で暗号化することができる。

【００３４】請求項４に記載の発明は、送信側では、蓄積した番組を視聴するときに用いる暗号鍵を番組ごとに更新するようにしたものであり、暗号鍵の１つが不正に解かれた場合でも、蓄積されている他の番組は不正視聴から免れることができる。

【００３５】請求項５に記載の発明は、受信側では、リアルタイムで番組を視聴するときに用いる暗号鍵を第１の種類のマスタ鍵で復号化して保持し、放送番組をリアルタイムで視聴するときには、復号化したこの暗号鍵を用いて、暗号化されたスクランブル鍵を復号化し、復号化したスクランブル鍵を用いて番組データのスクランブルを解除するようにしたものであり、リアルタイムでの番組視聴が可能となる。

【００３６】請求項６に記載の発明は、受信側では、蓄積した番組を視聴するときに用いる暗号鍵を第２の種類のマスタ鍵で復号化して保持し、蓄積した番組を再生して視聴するときには、復号化したこの暗号鍵を用いて、蓄積されている暗号化されたスクランブル鍵を復号化し、復号化したスクランブル鍵を用いて再生する番組データのスクランブルを解除するようにしたものであり、蓄積された番組の再生視聴が可能となる。

【００３７】請求項７に記載の発明は、送信側では、第２の種類のマスタ鍵を、第１の種類のマスタ鍵で暗号化して送信するようにしたものであり、蓄積番組視聴用の暗号鍵の復号化に用いるマスタ鍵を、放送を通じて配布することができ、このマスタ鍵を変更することが容易になる。

【００３８】請求項８に記載の発明は、受信側では、暗

号化されて送られて来る第２の種類のマスタ鍵を、第１の種類のマスタ鍵で復号化して保持するようにしたものであり、蓄積番組視聴用の暗号鍵の復号化に用いるマスタ鍵を、放送を通じて取得することができる。

【００３９】請求項９に記載の発明は、第１の種類のマスタ鍵を、各受信側に個別に設定し、第２の種類のマスタ鍵を、各受信側に共通に設定するようにしたものであり、蓄積番組視聴用の暗号鍵が各受信側に共通に設定したマスタ鍵で暗号化されるため、暗号化に多くの時間を必要とせず、更新間隔を短くすることができる。

【００４０】請求項１０に記載の発明は、受信側が放送番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムの送信装置において、第１の種類の暗号鍵を生成管理する第１の暗号鍵管理手段と、第２の種類の暗号鍵を生成管理する第２の暗号鍵管理手段と、番組データを暗号化したスクランブル鍵を第１の種類の暗号鍵で暗号化する第１のスクランブル鍵暗号化手段と、番組データを暗号化したスクランブル鍵を第２の種類の暗号鍵で暗号化する第２のスクランブル鍵暗号化手段と、第１の種類の暗号鍵を第１の種類のマスタ鍵で暗号化する第１の暗号鍵暗号化手段と、第２の種類の暗号鍵を第２の種類のマスタ鍵で暗号化する第２の暗号鍵暗号化手段と、第１のスクランブル鍵暗号化手段で暗号化されたスクランブル鍵、第２のスクランブル鍵暗号化手段で暗号化されたスクランブル鍵、第１の暗号鍵暗号化手段で暗号化された暗号鍵、第２の暗号鍵暗号化手段で暗号化された暗号鍵、及びスクランブル鍵で暗号化された番組データを多重化して送信する送信手段とを設けたものであり、番組データのスクランブルを解くスクランブル鍵が、複数種類の暗号鍵で暗号化されて送信される。

【００４１】請求項１１に記載の発明は、第２の暗号鍵管理手段が生成管理する第２の種類の暗号鍵の更新期間が、第１の暗号鍵管理手段が生成管理する第１の種類の暗号鍵の更新期間より短くなるようにしたものであり、番組データのスクランブルを解くスクランブル鍵が、更新期間を異にする複数種類の暗号鍵で暗号化されて送信される。

【００４２】請求項１２に記載の発明は、第２の種類のマスタ鍵を第１の種類のマスタ鍵で暗号化するマスタ鍵暗号化手段を設け、マスタ鍵暗号化手段で暗号化されたマスタ鍵を送信手段を通じて送信するようにしたものであり、蓄積番組視聴用の暗号鍵の復号化に用いるマスタ鍵を、放送を通じて各受信装置に配布することができる。

【００４３】請求項１３に記載の発明は、第１の種類のマスタ鍵を各受信装置ごとに設定し、第２の種類のマスタ鍵を各受信装置に共通に設定するようにしたものであり、蓄積番組の視聴に用いる暗号鍵の暗号化を短時間で行なうことが可能になる。

【００４４】請求項１４に記載の発明は、送信装置から放送された番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムの受信装置において、暗号化されている第１の種類の暗号鍵を第１の種類のマスタ鍵を用いて復号化する第１の暗号鍵復号手段と、暗号化されている第２の種類の暗号鍵を第２の種類のマスタ鍵を用いて復号化する第２の暗号鍵復号手段と、スクランブル鍵で暗号化された番組データと第２の種類の暗号鍵で暗号化されたスクランブル鍵とを記憶する蓄積手段と、第１の暗号鍵復号手段で復号化された暗号鍵を用いて、現在の受信情報に含まれる暗号化されたスクランブル鍵を復号化する第１のスクランブル鍵復号手段と、第２の暗号鍵復号手段で復号化された暗号鍵を用いて、蓄積手段から読み出した暗号化されているスクランブル鍵を復号化する第２のスクランブル鍵復号手段と、第１のスクランブル鍵復号手段または第２のスクランブル鍵復号手段で復号化されたスクランブル鍵を用いて番組データをデスクランブルするデスクランブラとを設けたものであり、番組をリアルタイム視聴する場合、または、蓄積した番組を再生視聴する場合に、異なる暗号鍵を用いてスクランブル鍵の復号化が行なわれる。

【００４５】請求項１５に記載の発明は、第２の暗号鍵復号手段で復号化される第２の種類の暗号鍵の更新期間が、第１の暗号鍵復号手段で復号化される第１の種類の暗号鍵の更新期間より短くなるようにしたものであり、更新期間が長い暗号鍵を用いて、番組をリアルタイム視聴するときのスクランブル鍵が復号化され、更新期間が短い暗号鍵を用いて、蓄積した番組を再生視聴するときのスクランブル鍵が復号化される。

【００４６】請求項１６に記載の発明は、デスクランブラが、番組をリアルタイム視聴するときには、現在受信しているスクランブルされている番組データを、第１のスクランブル鍵復号手段で復号されたスクランブル鍵を用いてデスクランブルし、蓄積された番組を再生して視聴するときには、蓄積手段から読み出したスクランブルされている番組データを、第２のスクランブル鍵復号手段で復号されたスクランブル鍵を用いてデスクランブルするようにしたものであり、番組をリアルタイム視聴するときと、蓄積した番組を再生視聴するときとでは、異なる種類の暗号鍵で復号化されたスクランブル鍵を用いて、番組データのスクランブルが解除される。

【００４７】請求項１７に記載の発明は、暗号化されている第２の種類のマスタ鍵を、第１の種類のマスタ鍵を用いて復号化するマスタ鍵復号手段を設け、マスタ鍵復号手段で復号化されたマスタ鍵を保持するようにしたものであり、蓄積番組視聴用の暗号鍵の復号化に用いるマスタ鍵を、放送を通じて取得することができる。

【００４８】請求項１８に記載の発明は、第１の種類のマスタ鍵が、各受信装置ごとに設定され、第２の種類のマスタ鍵が、各受信装置に共通に設定されるようにした

ものであり、各受信装置では、蓄積番組の視聴に用いる暗号鍵を、共通のマスタ鍵を使用して復号化する。

【００４９】以下、本発明の実施の形態について、図面を用いて説明する。

【００５０】（第１の実施形態）第１の実施形態の蓄積型放送システムでは、番組データにスクランブルを掛けるスクランブル鍵Ｋｓが、更新間隔を異にする２種類の暗号鍵で暗号化される。一方の暗号鍵は、従来の暗号鍵と同様、更新間隔が１年程度であり、この暗号鍵で暗号化されたＫｓは、受信装置で、番組をリアルタイムで視聴するときに復号化され、番組データのデスクランブルに使用される。この暗号鍵をリアルタイム系暗号鍵と言う。他方の暗号鍵は、番組ごとに更新され、この暗号鍵で暗号化されたＫｓは、受信装置で、蓄積された番組を視聴するときに復号化され、番組データのデスクランブルに使用される。この暗号鍵を蓄積系暗号鍵と言う。

【００５１】リアルタイム系暗号鍵は、受信装置ごとに異なるマスタ鍵で暗号化されて送信される。このリアルタイム系暗号鍵の暗号化に用いるマスタ鍵をリアルタイム系マスタ鍵と言う。一方、蓄積系暗号鍵は、各受信装置に共通のマスタ鍵で暗号化されて送信される。この蓄積系暗号鍵の暗号化に用いるマスタ鍵を蓄積系マスタ鍵と言う。

【００５２】このシステムの送信装置は、図１に示すように、番組データ（Data）を生成し管理する番組管理部41と、Dataを暗号化するためのスクランブル鍵Ｋｓを生成し管理するスクランブル鍵管理部42と、リアルタイム系暗号鍵Ｋw1を、その識別子（Kw1_ID）と共に生成管理するリアルタイム系暗号鍵管理部43と、リアルタイム系マスタ鍵Ｋm1を、その識別子（Km1_ID）と共に生成し管理するリアルタイム系マスタ鍵管理部44と、蓄積系暗号鍵Ｋw2を、その識別子（Kw2_ID）と共に生成管理する蓄積系暗号鍵管理部45と、蓄積系マスタ鍵Ｋm2を、その識別子（Km2_ID）と共に生成し管理する蓄積系マスタ鍵管理部46と、DataをＫｓでスクランブルし、スクランブル化された番組データData'を出力するスクランブラ47と、リアルタイム系暗号鍵Ｋw1の鍵本体を使ってＫｓを暗号化し、リアルタイム系暗号化スクランブル鍵Ｋs'1を出力するリアルタイム系スクランブル鍵暗号部48と、リアルタイム系マスタ鍵Ｋm1の鍵本体を使ってＫw1を暗号化し、リアルタイム系暗号化暗号鍵Kw1'を出力するリアルタイム系暗号鍵暗号部49と、蓄積系暗号鍵Ｋw2の鍵本体を使ってＫｓを暗号化し、蓄積系暗号化スクランブル鍵Ｋs'2を出力する蓄積系スクランブル鍵暗号部50と、蓄積系マスタ鍵Ｋm2の鍵本体を使ってＫw2を暗号化し、蓄積系暗号化暗号鍵Kw2'を出力する蓄積系暗号鍵暗号部51と、Data'、Ｋs'1、Kw1'、Ｋs'2及びKw2'を多重化し、多重化情報として出力する多重化部52と、多重化情報を伝送情報に変換して送信する送信部53とを備えている。

【００５３】この送信装置では、番組管理部41で生成されたDataが、スクランブラ47でスクランブル鍵Ｋｓを使ってスクランブルされ、スクランブル化された番組データData'が多重化部52に出力される。

【００５４】リアルタイム系暗号鍵管理部43では、生成したリアルタイム系暗号鍵Ｋw1を識別子Kw1_IDとともに、Ｋw1(Kw1_ID、Ｋw1本体）の形式で生成管理し、また、蓄積系暗号鍵管理部45では、番組ごとに生成した蓄積系暗号鍵Ｋw2を識別子Kw2_IDとともに、Ｋw2(Kw2_ID、Ｋw2本体）の形式で生成管理している。

【００５５】リアルタイム系スクランブル鍵暗号部48は、Dataのスクランブルで用いたＫsを、リアルタイム系暗号鍵管理部43から出力されたＫw1の鍵本体を使って暗号化し、暗号化に用いたＫw1の識別子Kw1_IDを付加して、リアルタイム系暗号化スクランブル鍵をＫs'1(Kw1_ID、Ｋs'1本体）の形式で多重化部52に出力する。また、蓄積系スクランブル鍵暗号部50は、Ｋsを蓄積系暗号鍵管理部45から出力されたＫw2の鍵本体を使って暗号化し、暗号化に用いたＫw2の識別子Kw2_IDを付加して、蓄積系暗号化スクランブル鍵をＫs'2(Kw2_ID、Ｋs'2本体）の形式で多重化部52に出力する。

【００５６】リアルタイム系マスタ鍵管理部44では、生成したリアルタイム系マスタ鍵を、識別子と共にＫm1(Km1_ID、Ｋm1本体）の形式で管理し、また、蓄積系マスタ鍵管理部46では、生成した蓄積系マスタ鍵を、識別子と共にＫm2(Km2_ID、Ｋm2本体）の形式で管理している。

【００５７】リアルタイム系暗号鍵暗号部49は、リアルタイム系暗号鍵の更新時期にＫw1(Kw1_ID、Ｋw1本体）をＫm1の鍵本体を使って暗号化し、暗号化に用いたＫm1の識別子Km1_IDを付加して、リアルタイム系暗号化暗号鍵をＫw1'(Km1_ID、Kw1_ID'、Ｋw1'本体）の形式で多重化部52に出力する。

【００５８】また、蓄積系暗号鍵暗号部51は、番組の送出に合わせて、Ｋw2(Kw2_ID、Ｋw2本体）をＫm2の鍵本体を使って暗号化し、暗号化に用いたＫm2の識別子Km2_IDを付加して、蓄積系暗号化暗号鍵をＫw2'(Km2_ID、Kw2_ID'、Ｋw2'本体）の形式で多重化部52に出力する。

【００５９】多重化部52は、入力するData'、Ｋs'1(Kw1_ID、Ｋs'1本体）、Ｋs'2(Kw2_ID、Ｋs'2本体）、Ｋw1'(Km1_ID、Kw1_ID'、Ｋw1'本体）及びＫw2'(Km2_ID、Kw2_ID'、Ｋw2'本体）を多重化して、その多重化情報を送信部53に出力し、送信部53は、それを伝送情報に変換して送信する。

【００６０】一方、受信装置は、図２に示すように、受信した伝送情報を多重情報に変換して出力するチューナー61と、チューナー61から出力された多重化情報を暗号化番組データData'、リアルタイム暗号化スクランブル鍵Ｋs'1、蓄積系暗号化スクランブル鍵Ｋs'2、リアルタイム系暗号化暗号鍵Ｋw1'及び蓄積系暗号化暗号鍵Ｋw2'

に分離して出力する分離部62と、Data'を蓄積する番組データ蓄積部64とＫｓ'2を蓄積するスクランブル鍵蓄積部65とを具備する蓄積媒体76と、分離部62で分離されたData'とＫｓ'2とを対応をとって番組データ蓄積部64及びスクランブル鍵蓄積部65に書き込む書き込み管理部63と、蓄積されているData'とＫｓ'2とを番組データ蓄積部64及びスクランブル鍵蓄積部65から取り出して出力する読み込み管理部66と、各受信装置によって異なるリアルタイム系マスタ鍵Ｋm1を蓄積しているリアルタイム系マスタ鍵蓄積部70と、Ｋm1を使ってＫw1'を復号化し、復号化されたＫw1を出力するリアルタイム系暗号鍵復号部69と、リアルタイム系暗号鍵復号部69から入力するＫw1を蓄積管理するリアルタイム系暗号鍵管理部71と、分離部62から入力するＫｓ'1をリアルタイム系暗号鍵管理部71から取り出したＫw1で復号化してＫｓを出力するリアルタイム系スクランブル鍵復号部72と、各受信装置に共通の蓄積系マスタ鍵Ｋm2を蓄積している蓄積系マスタ鍵蓄積部79と、Ｋm2を使ってＫw2'を復号化し、復号化されたＫw2を出力する蓄積系暗号鍵復号部78と、蓄積系暗号鍵復号部78から入力するＫw2を蓄積管理する蓄積系暗号鍵管理部80と、読み込み管理部66から入力するＫｓ'2を蓄積系暗号鍵管理部80から取り出したＫw2で復号化してＫｓを出力する蓄積系スクランブル鍵復号部81と、リアルタイムで視聴するときは分離部62からData'を選択し、蓄積された番組を視聴するときは読み込み管理部66からData'を選択する番組データ選択部67と、リアルタイムで視聴するときはリアルタイム系スクランブル鍵復号部72で復号化されたＫｓを選択し、蓄積された番組を視聴するときは蓄積系スクランブル鍵復号部81で復号化されたＫｓを選択するスクランブル鍵選択部68と、番組データ選択部67から入力するData'をスクランブル鍵選択部68から入力するＫｓで復号化してDataを出力するデスクランブラ73と、Dataを再生信号にデコードするデコーダ74と、再生信号に基づいて番組表示を行なう表示装置75とを備えている。また、リアルタイム系マスタ鍵蓄積部70、リアルタイム系暗号鍵復号部69、リアルタイム系暗号鍵管理部71、リアルタイム系スクランブル鍵復号部72、蓄積系マスタ鍵蓄積部79、蓄積系暗号鍵復号部78、蓄積系暗号鍵管理部80及び蓄積系スクランブル鍵復号部81はセキュリティモジュール77に設けられており、このセキュリティモジュール77は、放送局から配布され受信装置にセットされる。従って、リアルタイム系マスタ鍵及び蓄積系マスタ鍵は、このセキュリティモジュール77を通じて各受信装置に与えられる。

【００６１】この受信装置では、分離部62が、チューナー61から入力する多重化情報を、暗号化番組データData'、リアルタイム系暗号化スクランブル鍵Ｋｓ'1(Kw1_ID、Ｋｓ'1本体)、蓄積系暗号化スクランブル鍵Ｋｓ'2(Kw2_ID、Ｋｓ'2本体)、リアルタイム系暗号化暗号鍵Ｋw1'(Km1_ID、Kw1_ID'、Ｋw1'本体)及び蓄積系暗号化暗号鍵Ｋw2'(Km2_ID、Kw2_ID'、Ｋw2'本体)に分離して出力する。書き込み管理部63は、分離部62から分離されたData'とＫｓ'2とを対応をとって蓄積媒体76の番組データ蓄積部64及びスクランブル鍵蓄積部65に書き込む。

【００６２】また、リアルタイム系暗号鍵復号部69は、リアルタイム系マスタ鍵蓄積部70に蓄積されているリアルタイム系マスタ鍵Ｋm1(Km1_ID、Ｋm1本体)と同一のKm1_IDをもつリアルタイム系暗号化暗号鍵Ｋw1'(Km1_ID、Kw1_ID'、Ｋw1'本体)が分離部62から出力されたとき、そのＫm1を使ってＫw1'を復号化し、復号化したリアルタイム系復号化暗号鍵Ｋw1(Kw1_ID、Ｋw1本体)をリアルタイム系暗号鍵管理部71に出力する。リアルタイム系暗号鍵管理部71は、これを蓄積管理する。

【００６３】また、蓄積系暗号鍵復号部78は、蓄積系マスタ鍵蓄積部79に蓄積されている蓄積系マスタ鍵Ｋm2(Km2_ID、Ｋm2本体)と同一のKm2_IDをもつ蓄積系暗号化暗号鍵Ｋw2'(Km2_ID、Kw2_ID'、Ｋw2'本体)が分離部62から出力されたとき、そのＫm2を使ってＫw2'を復号化し、復号化した蓄積系復号化暗号鍵Ｋw2(Kw2_ID、Ｋw2本体)を蓄積系暗号鍵管理部80に出力する。蓄積系暗号鍵管理部80は、これを蓄積管理する。

【００６４】視聴者からリアルタイムの番組視聴が指示された場合には、番組データ選択部67は、分離部62からData'を入手してデスクランブラ73に出力する。また、リアルタイム系スクランブル鍵復号部72は、分離部62からＫｓ'1(Kw1_ID、Ｋｓ'1本体)が入力すると、リアルタイム系暗号鍵管理部71からＫｓ'1と同一のKw1_IDを持つＫw1(Kw1_ID、Ｋw1本体)を取り出し、それを使ってＫｓを復号化する。

【００６５】番組データ選択部67と連動するスクランブル鍵選択部68は、リアルタイム系スクランブル鍵復号部72で復号化されたＫｓを選択してデスクランブラ73に出力する。デスクランブラ73は、このＫｓを使って番組データ選択部67から入力するData'を復号化し、Dataをデコーダ74に出力する。

【００６６】一方、視聴者から蓄積番組の視聴が指示された場合には、読み込み管理部66は、番組データ蓄積部64から、蓄積されている指示された番組のData'を読み出すとともに、そのData'のスクランブルを行なっているＫｓ'2(Kw2_ID、Ｋｓ'2本体)をスクランブル鍵蓄積部65から取り出す。

【００６７】番組データ選択部67は、読み込み管理部66からData'を入手してデスクランブラ73に出力する。また、蓄積系スクランブル鍵復号部81は、読み込み管理部66で読み出されたＫｓ'2(Kw2_ID、Ｋｓ'2本体)を入手し、蓄積系暗号鍵管理部80からＫｓ'2と同一のKw2_IDを持つＫw2(Kw2_ID、Ｋw2本体)を取り出し、それを使ってＫｓを復号化する。

【００６８】番組データ選択部67と連動するスクランブル鍵選択部68は、蓄積系スクランブル鍵復号部81で復号

化されたＫｓを選択してデスクランブラ73に出力する。デスクランブラ73は、このＫｓを使って番組データ選択部67から入力するData'を復号化し、Dataをデコーダ74に出力する。

【００６９】このように、この蓄積型放送システムでは、スクランブル鍵Ｋｓが、更新間隔が長いリアルタイム系暗号鍵と、番組ごとに更新される蓄積系暗号鍵とを用いて暗号化され、また、リアルタイム系暗号鍵は、各受信装置ごとに異なるリアルタイム系マスタ鍵で暗号化され、蓄積系暗号鍵は、各受信装置に共通の蓄積系マスタ鍵で暗号化される。

【００７０】受信装置では、暗号化されたリアルタイム系暗号鍵をリアルタイム系マスタ鍵で復号化し、今まで保持していた鍵に替えて、新たに復号化したリアルタイム系暗号鍵を保持管理する。また、暗号化された蓄積系暗号鍵を蓄積系マスタ鍵で復号化し、これまで保持していた蓄積系暗号鍵と併せて、新たに復号化した蓄積系暗号鍵を保持管理する。

【００７１】また、蓄積媒体には、スクランブル鍵でスクランブルされた番組データと、蓄積系暗号鍵で暗号化されたスクランブル鍵とを蓄積する。

【００７２】放送番組をリアルタイムで視聴するときは、保持管理しているリアルタイム系暗号鍵を用いて、リアルタイム系暗号鍵で暗号化されているスクランブル鍵を復号化し、復号化したスクランブル鍵で番組データをデスクランブルする。

【００７３】また、蓄積した番組の再生時には、再生する番組に合わせて、保持管理している蓄積系暗号鍵の中から、使用する蓄積系暗号鍵を選択し、その蓄積系暗号鍵で暗号化されているスクランブル鍵を復号化し、復号化したスクランブル鍵で、再生する番組データをデスクランブルする。

【００７４】受信装置の蓄積媒体には多数の番組が蓄積されるが、しかし、これらの番組のスクランブルを解くためのスクランブル鍵は、各番組ごとに異なる種類の蓄積系暗号鍵で暗号化されているため、ある番組で用いた蓄積系暗号鍵が不正に解かれたとしても、その他の番組は、不正視聴の対象から免れることができる。

【００７５】また、放送送信装置では、暗号化した蓄積系暗号鍵を番組ごとに各受信装置に送信しなければならないが、この暗号化には各受信装置に共通のマスタ鍵を使用しているため、暗号化処理に費やす時間は短くて済み、そのため、更新間隔を短縮することが可能となる。

【００７６】なお、ここでは、蓄積系暗号鍵を番組ごとに更新する場合について説明したが、この更新の間隔は、日、週あるいは月単位などで更新するようにしてもよい。また、蓄積系暗号鍵の更新間隔をリアルタイム系暗号鍵の更新間隔と同じにした場合でも、番組をリアルタイム視聴するときの暗号鍵と蓄積した番組を視聴するときの暗号鍵とが違うために、暗号が不正解読されたときの被害の範囲を狭めることができる。

【００７７】また、本発明は、番組を自動蓄積する蓄積型の放送システムや、視聴者の選択に基づいて放送番組が蓄積されるシステムなどに適用することができる。

【００７８】（第２の実施形態）第２の実施形態の蓄積型放送システムでは、各受信装置に共通に設定する蓄積系マスタ鍵を、放送を通じて各受信装置に配布している。

【００７９】このシステムの送信装置は、図３に示すように、リアルタイム系マスタ鍵管理部104で生成されたリアルタイム系マスタ鍵Ｋm1の鍵本体を使って蓄積系マスタ鍵管理部106で生成された蓄積系マスタ鍵Ｋm2を暗号化する蓄積系マスタ鍵暗号部114を備えており、多重化部112は、蓄積系マスタ鍵暗号部114で暗号化された蓄積系暗号化マスタ鍵Ｋm2'(Km1_ID、Km2_ID'、Km2'本体）をData'、Ｋs'1、Ｋs'2、Ｋw1'及びＫw2'とともに多重化し、多重化情報として出力する。その他の構成は第１の実施形態の送信装置（図１）と変わりがない。

【００８０】一方、このシステムの受信装置は、図４に示すように、リアルタイム系マスタ鍵蓄積部210に蓄積されているリアルタイム系マスタ鍵Ｋm1を使って、分離部202で分離された蓄積系暗号化マスタ鍵Ｋm2'を復号化し、復号化された蓄積系マスタ鍵Ｋm2を出力する蓄積系マスタ鍵復号部222を備えており、蓄積系マスタ鍵復号部222で復号された蓄積系マスタ鍵Ｋm2が、蓄積系マスタ鍵蓄積部219に蓄積される。その他の構成は第１の実施形態の受信装置（図２）と変わりがない。

【００８１】このシステムでは、蓄積系暗号鍵Ｋw2の暗号化に用いられる各受信装置に共通の蓄積系マスタ鍵Ｋm2が、各受信装置に割り当てたリアルタイム系マスタ鍵Ｋm1を使って暗号化され、それぞれの受信装置に送信される。

【００８２】各受信装置では、暗号化されている蓄積系マスタ鍵Ｋm2'を、セキュリティモジュール217で保持しているリアルタイム系マスタ鍵Ｋm1を使って復号化し、蓄積系マスタ鍵蓄積部219に格納する。蓄積系暗号鍵Ｋw2は、この蓄積系マスタ鍵Ｋm2を使って復号化される。

【００８３】このように、このシステムでは、リアルタイム系マスタ鍵Ｋm1は、セキュリティモジュール217の配布を通じて各受信装置に与えられ、一方、蓄積系マスタ鍵Ｋm2は、放送を通じて各受信装置に与えられる。そのため、各受信装置に共通に設定する蓄積系マスタ鍵Ｋm2の変更を容易に行なうことができ、この蓄積系マスタ鍵を適宜変更することにより、蓄積系暗号鍵の不正解読を困難にすることができる。

【００８４】

【発明の効果】以上の説明から明らかなように、本発明の放送システムでは、番組のリアルタイム視聴の際に用いる暗号鍵と、蓄積した番組を再生視聴する際に用いる

暗号鍵との種類を違えており、また、後者の蓄積系暗号鍵の更新間隔を短く設定しているため、暗号鍵の不正解読による被害を小さい範囲に止めることができる。

【００８５】例えば、蓄積系暗号鍵を番組単位で変更する場合には、１つの暗号鍵が不正に解かれても、不正視聴できる番組は１つに限られ、蓄積されている他の番組データの視聴を制限することができる。

【００８６】また、本発明の送信装置及び受信装置は、この放送システムを実現することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態における放送システムの送信装置の構成を示すブロック図、

【図２】本発明の第１の実施形態における放送システムの受信装置の構成を示すブロック図、

【図３】本発明の第２の実施形態における放送システムの送信装置の構成を示すブロック図、

【図４】本発明の第２の実施形態における放送システムの受信装置の構成を示すブロック図、

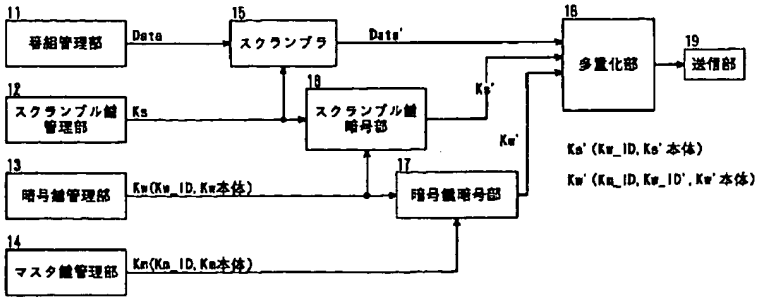
【図５】従来の送信装置の構成を示すブロック図、

【図６】従来の受信装置の構成を示すブロック図である。

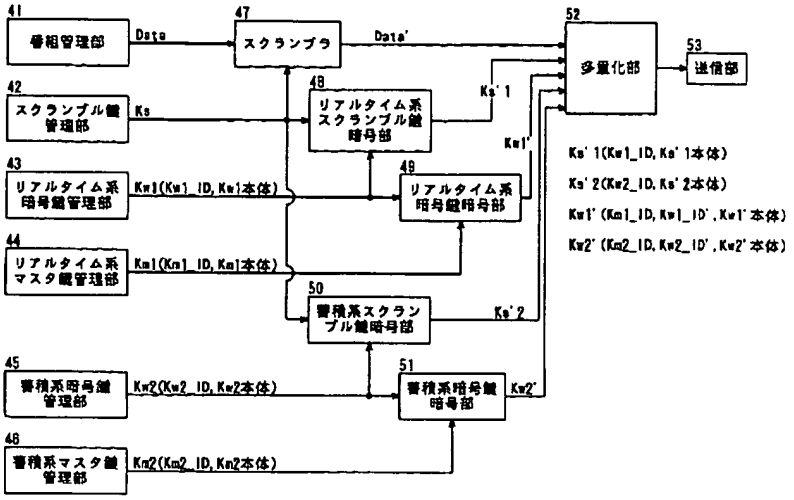
【符号の説明】

11、41、101　番組管理部
12、42、102　スクランブル鍵管理部
13　暗号鍵管理部
14　マスタ鍵管理部
15、47、107　スクランブラ
16　スクランブル鍵暗号部
17　暗号鍵暗号部
18、52、112　多重化部
19、53、113　送信部
21、61、201　チューナー
22、62、202　分離部
＊23、63、203　書き込み管理部
24、64、204　番組データ蓄積部
25、65、205　スクランブル鍵蓄積部
26、66、206　読み込み管理部
27、67、207　番組データ選択部
28、68、208　スクランブル鍵選択部
29　暗号鍵復号部
30　マスタ鍵蓄積部
31　暗号鍵管理部
32　スクランブル鍵復号部
33、73、213　デスクランブラ
34、74、214　デコーダ
35、75、215　表示装置
36、76、216　蓄積媒体
37、77、217　セキュリティモジュール
43、103　リアルタイム系暗号鍵管理部
44、104　リアルタイム系マスタ鍵管理部
45、105　蓄積系暗号鍵管理部
46、106　蓄積系マスタ鍵管理部
48、108　リアルタイム系スクランブル鍵暗号部
49、109　リアルタイム系暗号鍵暗号部
50、110　蓄積系スクランブル鍵暗号部
51、111　蓄積系暗号鍵暗号部
69、209　リアルタイム系暗号鍵復号部
70、210　リアルタイム系マスタ鍵蓄積部
71、211　リアルタイム系暗号鍵管理部
72、212　リアルタイム系スクランブル鍵復号部
78、218　蓄積系暗号鍵復号部
79、219　蓄積系マスタ鍵蓄積部
80、220　蓄積系暗号鍵管理部
81、221　蓄積系スクランブル鍵復号部
114　蓄積系マスタ鍵暗号部
＊222　蓄積系マスタ鍵復号部

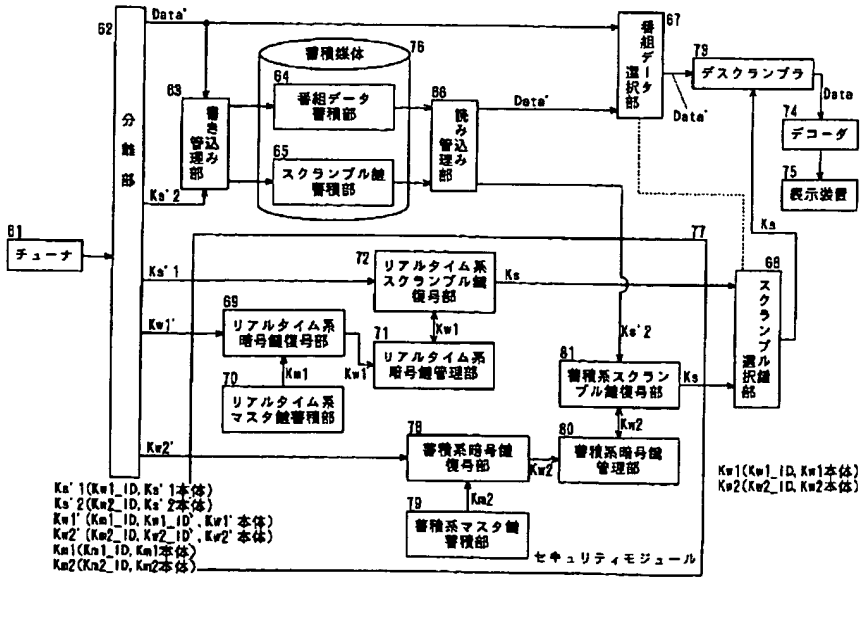
【図５】



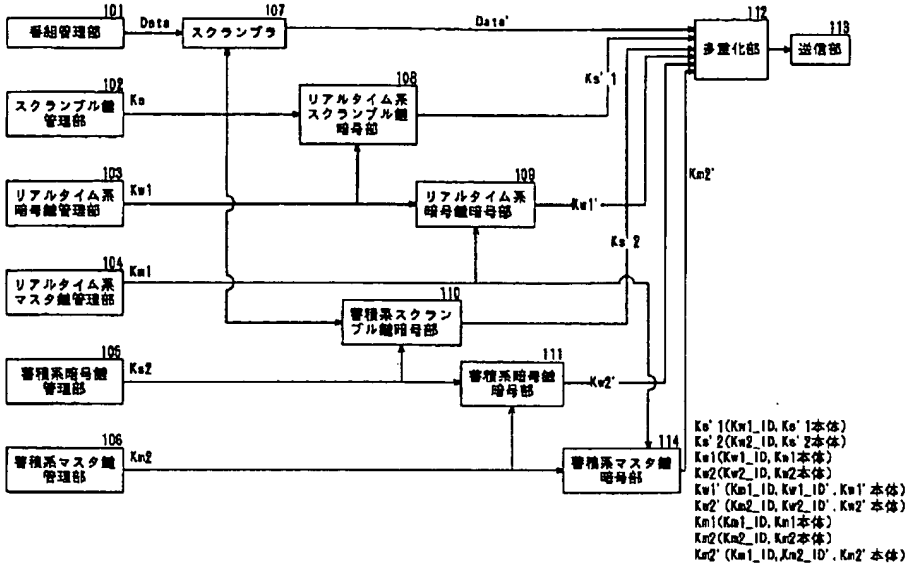
【図１】


41
番組管理部
Data
47
スクランブラ
Data'
52
多重化部
53
送信部
42
スクランブル鍵管理部
Ks
48
リアルタイム系スクランブル鍵暗号部
Ks'1
Kw1'
43
リアルタイム系暗号鍵管理部
Kw1(Kw1_ID, Kw1本体)
49
リアルタイム系暗号鍵暗号部
44
リアルタイム系マスタ鍵管理部
Km1(Km1_ID, Km1本体)
50
蓄積系スクランブル鍵暗号部
Ks'2
45
蓄積系暗号鍵管理部
Kw2(Kw2_ID, Kw2本体)
51
蓄積系暗号鍵暗号部
Kw2'
46
蓄積系マスタ鍵管理部
Km2(Km2_ID, Km2本体)
Ks'1(Kw1_ID, Ks'1本体)
Ks'2(Kw2_ID, Ks'2本体)
Kw1'(Km1_ID, Kw1_ID', Kw1'本体)
Kw2'(Km2_ID, Kw2_ID', Kw2'本体)

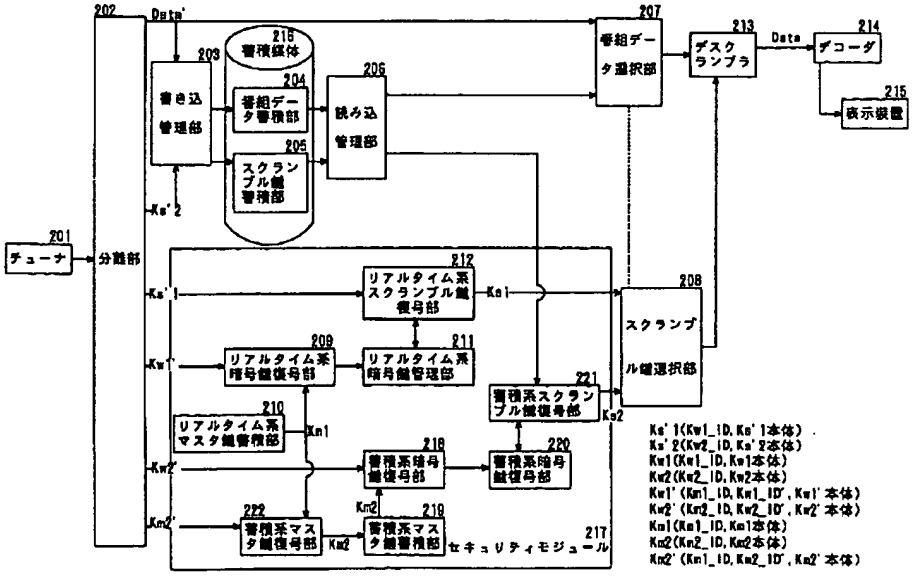
【図２】


62
分離部
Data'
63
書き込み管理部
64
番組データ蓄積部
65
スクランブル鍵蓄積部
蓄積媒体
76
66
読み出し管理部
67
番組データ選択部
79
デスクランブラ
Data
74
デコーダ
75
表示装置
61
チューナ
Ks'1
Kw1'
Ks'2
Kw2'
72
リアルタイム系スクランブル鍵復号部
Ks
69
リアルタイム系暗号鍵復号部
Kw1
71
リアルタイム系暗号鍵管理部
Km1
70
リアルタイム系マスタ鍵蓄積部
77
68
スクランブル選択鍵部
81
蓄積系スクランブル鍵復号部
Kw2
78
蓄積系暗号鍵復号部
80
蓄積系暗号鍵管理部
Km2
79
蓄積系マスタ鍵蓄積部
セキュリティモジュール
Ks'1(Kw1_ID, Ks'1本体)
Ks'2(Kw2_ID, Ks'2本体)
Kw1'(Km1_ID, Kw1_ID', Kw1'本体)
Kw2'(Km2_ID, Kw2_ID', Kw2'本体)
Km1(Km1_ID, Km1本体)
Km2(Km2_ID, Km2本体)
Kw1(Kw1_ID, Kw1本体)
Kw2(Kw2_ID, Kw2本体)

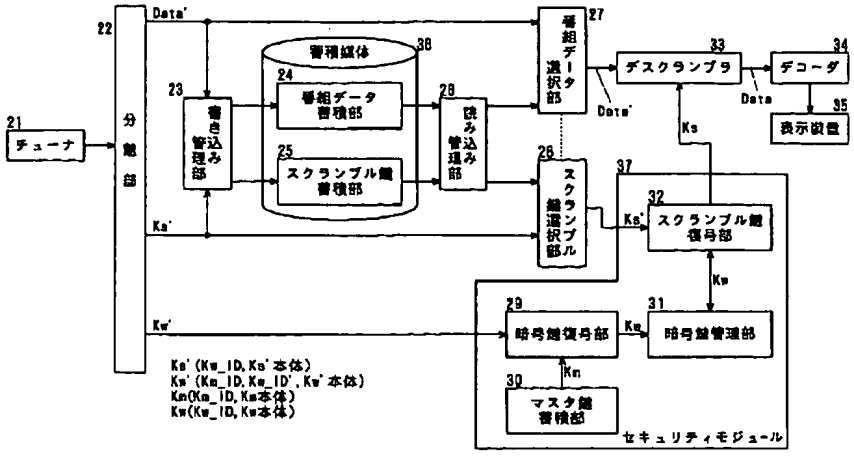
【図３】


101
番組管理部
Data
107
スクランブラ
Data'
112
多重化部
113
送信部
102
スクランブル鍵管理部
Ks
108
リアルタイム系スクランブル鍵暗号部
Ks'1
103
リアルタイム系暗号鍵管理部
Kw1
109
リアルタイム系暗号鍵暗号部
Kw1'
Km2'
Ks'2
104
リアルタイム系マスタ鍵管理部
Km1
110
蓄積系スクランブル鍵暗号部
105
蓄積系暗号鍵管理部
Kw2
111
蓄積系暗号鍵暗号部
Kw2'
106
蓄積系マスタ鍵管理部
Km2
114
蓄積系マスタ鍵暗号部
Ks'1(Kw1_ID,Ks'1本体)
Ks'2(Kw2_ID,Ks'2本体)
Kw1(Kw1_ID,Kw1本体)
Kw2(Kw2_ID,Kw2本体)
Kw1'(Km1_ID,Kw1_ID',Kw1'本体)
Kw2'(Km2_ID,Kw2_ID',Kw2'本体)
Km1(Km1_ID,Km1本体)
Km2(Km2_ID,Km2本体)
Km2'(Km1_ID,Km2_ID',Km2'本体)

【図４】


202
Data'
216
蓄積媒体
207
番組データ選択部
213
デスクランブラ
Data
214
デコーダ
215
表示装置
203
書き込管理部
204
番組データ蓄積部
206
読み込管理部
205
スクランブル鍵蓄積部
Ks'2
201
チューナ
分離部
212
リアルタイム系スクランブル鍵復号部
Ks1
208
スクランブル鍵選択部
209
リアルタイム系暗号鍵復号部
211
リアルタイム系暗号鍵管理部
221
蓄積系スクランブル鍵復号部
Ks2
210
リアルタイム系マスタ鍵蓄積部
Km1
218
蓄積系暗号鍵復号部
220
蓄積系暗号鍵復号部
Km2
222
蓄積系マスタ鍵復号部
Km2
219
蓄積系マスタ鍵蓄積部
217
セキュリティモジュール
Ks'1(Kw1_ID,Ks'1本体)
Ks'2(Kw2_ID,Ks'2本体)
Kw1(Kw1_ID,Kw1本体)
Kw2(Kw2_ID,Kw2本体)
Kw1'(Km1_ID,Kw1_ID',Kw1'本体)
Kw2'(Km2_ID,Kw2_ID',Kw2'本体)
Km1(Km1_ID,Km1本体)
Km2(Km2_ID,Km2本体)
Km2'(Km1_ID,Km2_ID',Km2'本体)

【図６】



フロントページの続き

(72)発明者　原田　武之助
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　町田　和弘
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　片岡　充照
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　5C064 CA14 CA18 CB01 CB08 CC04 CC06
5K013 AA01 BA02 BA04 BA05 EA02 FA06